



TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US)  
CONCERNING A FILING UNDER 35 USC 371

International Application No.: PCT/GB98/02064  
 International Filing Date: July 13, 1998  
 Priority Date Claimed: July 17, 1997  
 Title of Invention: ENCRYPTED BROADCAST MESSAGES IN A CELLULAR  
 COMMUNICATIONS SYSTEM  
 Applicant(s) for DO/EO/US: Peter Ford

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1.  This is a **FIRST** submission of items concerning a filing under 35 USC 371.
2.  This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 USC 371.
3.  This express request to begin national examination procedures (35 USC 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 USC 371(b) and PCT Articles 22 and 39(1).
4.  A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5.  A copy of the International Application as filed (35 USC 371(c)(2))
  - a)  is transmitted herewith (required only if not transmitted by the International Bureau).
  - b)  has been transmitted by the International Bureau.
  - c)  is not required, as the application was filed in the United States Receiving Office (RO/US).
6.  A translation of the International Application into English (35 USC 371(c)(2)).
7.  Amendments to the claims of the International Application under PCT Article 19 (35 USC 371(c)(3))
  - a)  are transmitted herewith (required only if not transmitted by the International Bureau).
  - b)  have been transmitted by the International Bureau.
  - c)  have not been made; however, the time limit for making such amendments has NOT expired.
  - d)  have not been made and will not be made.
8.  A translation of the amendments to the claims under PCT Article 19 (35 USC 371(c)(3)).
9.  An oath or declaration of the inventor(s) (35 USC 371(c)(4)).
10.  A copy of the International Preliminary Examination Report with any annexes thereto, such as any amendments made under PCT Article 34.
11.  A translation of the annexes, such as any amendments made under PCT Article 34, to the International Preliminary Examination Report under PCT Article 36 (35 USC 371(c)(5)).

U.S. Application No.  
Unknown

International Application No.  
PCT/GB98/02064

Date: January 18, 2000

09/463146

Attorney Docket No.  
RJENK9.001APC

420 Rec'd PCT/PTO 18 JAN 2000  
Page 2

**Items 11. to 16. below concern other document(s) or information included:**

12.  An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
13.  An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
14.  A FIRST preliminary amendment.  
 A SECOND or SUBSEQUENT preliminary amendment.
15.  A substitute specification.
16.  A power of attorney and/or address letter.
17.  International Application as published.
18.  Small Entity Statement.
19.  PCT Form PCT/IPEA/402.
20.  PCT Form PCT/IB/308.
21.  PCT request form.
22.  A return prepaid postcard.
23.  The following fees are submitted:

U.S. Application No.  
Unknown

International Application No.  
PCT/GB98/02064

Date: January 18, 2000

09/1463146

Attorney Docket No.  
RJENK9.001APC

420 Rec'd PCT/PTO 18 JAN 2000

Page 3

FEES

BASIC FEE		\$840		
CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE	
Total Claims	19 - 20 =	0 ×	\$18	\$0
Independent Claims	3 - 3 =	0 ×	\$78	\$0
Multiple dependent claims(s) (if applicable)			\$260	\$0

**TOTAL OF ABOVE CALCULATIONS \$0**

Reduction by 1/2 for filing by small entity (if applicable). Verified Small Entity \$0  
statement must also be filed. (NOTE 37 CFR 1.9, 1.27, 1.28)

**TOTAL NATIONAL FEE \$840**

**TOTAL FEES ENCLOSED \$840**

amount to be refunded: \$0  
amount to be charged: \$0

24.  The fee for later submission of the signed oath or declaration set forth in 37 CFR 1.492(e) will be paid upon submission of the declaration.

25.  A check in the amount of \$840 to cover the above fees is enclosed.

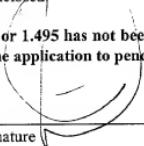
26.  Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). \$40 per property.

27.  The Commissioner is hereby authorized to charge only those additional fees which may be required to avoid abandonment of the application, or credit any overpayment to Deposit Account No. 11-1410. A duplicate copy of this sheet is enclosed.

**NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.**

SEND ALL CORRESPONDENCE TO:

KNOBBE, MARTENS, OLSON & BEAR, LLP  
620 Newport Center Drive  
Sixteenth Floor  
Newport Beach, CA 92660

  
Signature

John M. Carson  
Printed Name

34,303  
Registration Number

RJENK9.001APC

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	:	Peter Ford	)	Group Art Unit Unknown
			)	
Appl. No.	:	Unknown	)	
			)	
Filed	:	Herewith	)	
			)	
For	:	ENCRYPTED BROADCAST	)	
		MESSAGES IN A CELLULAR	)	
		COMMUNICATIONS	)	
		SYSTEM	)	
			)	
Examiner	:	Unknown	)	

PRELIMINARY AMENDMENT

Assistant Commissioner for Patents  
Washington, D.C. 20231

Dear Sir:

Prior to examination of the above-captioned application, please amend the application as follows:

IN THE CLAIMS:

Please cancel Claims 1-18 as amended during the International phase, without prejudice.

**Please add new Claims 19-37 as follows:**

19. A method of distributing information to users in a cellular telecommunications network comprising a plurality of base stations transceiving in a plurality of cells of the network, the method comprising:

providing a plurality of mobile stations, each of the mobile stations having an associated information access status;

Appl. No. : Unknown  
Filed : Herewith

broadcasting a signal on a common channel of at least one cell of the network, the signal containing a limited access message in encrypted form, for general reception in the at least one cell;

enabling first mobile stations having a first information access status to decrypt and present the message to a user in unencrypted form when being served by the cell; and

preventing second mobile stations having a second information access status from presenting the message in unencrypted form to a user when being served in the cell, wherein the first mobile stations are provided with a removable module which may be used in association with any of a plurality of mobile stations, the removable module storing a decryption key for the message, and wherein the message is decrypted, using the decryption key, in the removable module.

20. The method according to Claim 19, further comprising enabling both the first and second mobile stations to read a message identifier comprised in the signal and accompanying a message.

21. The method according to Claim 19, further comprising storing the decryption key in the removable module in encrypted form.

22. The method according to Claim 21, further comprising decrypting the decryption key by the first mobile station using a data string specific to the removable module.

23. The method according to Claim 22, wherein the data string is a subscriber identifier used in the cellular telecommunications network.

24. The method according to Claim 19, further comprising transmitting the decryption key to the first mobile stations via a radio interface in the cellular telecommunications network.

25. The method according to Claim 19, wherein the removable module is a subscriber identity module.

26. The method according to Claim 25, wherein the message includes a transfer protocol identifier indicating that the message is of a type for data download to the subscriber identity module from the mobile station.

27. The method according to Claim 19, further comprising storing in the removable module an application program for performing the decryption and for controlling a display of the message on the mobile station.

Appl. No. : Unknown  
Filed : Herewith

28. The method according to Claim 19, wherein the signal comprises a plurality of limited access messages each having a corresponding decryption key,

the method comprising providing the first mobile stations with the decryption keys, storing the decryption keys on removable modules of the first mobile stations, and enabling only ones of the first mobile stations having a decryption key corresponding to a limited access message to present the limited access message to a user in unencrypted form when being served in a cell.

29. The method according to Claim 28, further comprising providing each of the first mobile stations with a selection of the subscription keys in accordance with a subscription held for each first mobile station respectively.

30. The method according to Claim 19, wherein alternative limited access messages are broadcast in cells located in different areas of the cellular telecommunications network.

31. The method according to Claim 19, wherein the common channel is a cell broadcast channel of a GSM-type communications system.

32. A mobile station for receiving information in a cellular telecommunications system, the mobile station comprising:

means for receiving an encrypted message broadcast on a common channel of a cell of the cellular telecommunications system;

means for displaying the message, when decrypted, to a user; and

a removable module comprising a memory for storing a decryption key, and means for decrypting the message using the stored decryption key.

33. The mobile station according to Claim 32, wherein the removable module is a subscriber identity module.

34. The mobile station according to Claim 32, wherein the removable module stores an application program for performing the decryption and for controlling the display of the message on the mobile station.

35. The mobile station according to Claim 32, wherein the mobile station is configured to operate in accordance with GSM Phase 2+.

36. The mobile station according to Claim 32, wherein the mobile station is configured to operate as a cellular mobile telephone.

Appl. No. : Unknown  
Filed : Herewith

37. A mobile station for receiving information in a cellular telecommunications system, the mobile station comprising:

a receiver unit configured to receive an encrypted message broadcast on a common channel of a cell of the cellular telecommunications system;  
a display to display the message, when decrypted, to a user; and  
a removable module comprising a memory for storing a decryption key, and being configured to decrypt the message using the stored decryption key.

REMARKS

The foregoing amendments are to more closely conform the application to U.S. practice. No new matter is added. Entry of the amendments is respectfully requested.

Respectfully submitted,

KNOBBE, MARTENS, OLSON & BEAR, LLP

By: \_\_\_\_\_

John M. Carson

Registration No. 34,303

Attorney of Record

620 Newport Center Drive

Sixteenth Floor

Newport Beach, CA 92660

(619) 235-8550

Dated: 1/18/00

ENCRYPTED BROADCAST MESSAGES IN A CELLULAR COMMUNICATIONS SYSTEM

This invention relates to a method of an apparatus for distributing and receiving information in a cellular telecommunications network, for example a  
5      GSM (Global System for Mobile communications) digital cellular radio network.

The GSM standard is defined in a set of technical specifications issued by the European Telecommunications Standards Institute (ETSI), and there are currently a number of mobile telecommunications networks operating in  
10     accordance with the GSM standard, and variants thereof, such as the DCS1800 standard.

One service provided is a service referred to as a cell broadcast (CB), or short message - cell broadcast (SMS CB), service. In this service, information in the form of pages of text is transmitted on a common channel (the cell broadcast channel, CBCH) of cells in the network. The transmission of pages is repeated at regular intervals, and users can store the information for retrieval and display by means of selective keystrokes on a mobile station, or may turn off the cell broadcast function so as not to store the information. The information is intended to include locality-specific information, such as lists of local facilities (hospitals, pharmacies, taxis, etc), local weather reports, local  
15     date/time indications, etc.

At present, however, the cell broadcast functionality, although provided for in current GSM-type networks and the mobile stations used in them, has not been widely implemented in practice, in probability at least partly due to the costs associated with assembling and disseminating information via the service.

5 In accordance with an aspect of the present invention there is provided a method of distributing information to users in a cellular telecommunications network comprising a mobile switching centre and a plurality of base stations transceiving in a plurality of cells of said network, said method comprising:

10 providing a plurality of mobile stations, each of said mobile stations having an associated information access status;

broadcasting a signal on a common channel of at least one cell of said network, said signal containing a limited access message in encrypted form, for general reception in said at least one cell;

15 enabling first mobile stations having a first information access status to decrypt and present said message to a user in unencrypted form when being served by said cell; and

20 preventing second mobile stations having a second information access status from presenting said message in unencrypted form to a user when being served in said cell.

An advantage of this aspect of the invention is that a user not authorised to access the information can only view the message in encrypted form and unintelligibly, whereas a user having access rights to the information is able to

view the message in decrypted and intelligible form services may be provided on a subscription basis. Some subscribers in the network may wish to have access to the information broadcast generally in the cell in addition to other services provided in the telecommunications network, such as voice call services, and will take out a subscription allowing access to the cellular information broadcasting service. Other users may not wish to receive the benefit of the information broadcast in the cell, and will take out a subscription, perhaps at lower cost, preventing them from accessing the information.

Preferably, the signal comprises a plurality of limited access messages each having a corresponding access right, the method comprising providing mobile stations with access rights, and enabling only mobile stations having an access right corresponding to a limited access message to present the limited access message to a user when being served in the cell. This allows the selection on a per user basis of the type of information a user is able to access, thus allowing a subscription to be individually tailored to a subscribers' needs.

The signal may also contain a general access message, the method comprising enabling both the first and second mobile stations to present the general access message to a user when being served in the cell. This allows both limited access messages and general access messages to be disseminated by broadcasts in cells of a cellular telecommunications system, allowing some information to be presented to any user irrespective of the subscription type held.

Preferably, alternative limited access messages are broadcast in cells located in different areas of the cellular telecommunications network, thereby tailoring the information within the messages to different localities and increasing the utility of the service.

5 In accordance with a further aspect of the invention there is provided apparatus for receiving information in a cellular telecommunications system, said apparatus comprising:

means for storing a decryption key;

means for receiving a message on a common channel in a cell of said 10 cellular telecommunications system; and

means for decrypting said message using said stored decryption key; and

means for displaying said decrypted message to a user.

This aspect provides apparatus whereby a user may receive limited 15 access messages on a common channel of a cell in the telecommunications system, and view the information in decrypted form, if the mobile station of the user is provided with the decryption key. A decryption key may be distributed only to cellular users having a predetermined subscription type.

An embodiment of the present invention will now be described, by way of example only, with reference to the accompanying drawings, wherein:

20 Figure 1 is a block diagram schematically illustrating a cellular telecommunications system;

Figure 2 is a block diagram schematically illustrating a cellular telecommunicationsmobile station;

Figure 3 illustrates a list stored in a cell broadcast centre in accordance with the present invention;

5 Figure 4 is a flow diagram illustrating functions carried out by the cell broadcast centre in accordance with the present invention;

Figures 5 and 6 illustrate data blocks broadcast in a cell in accordance with the present invention;

10 Figure 7 is a flow diagram illustrating functions carried out by a network management centre in accordance with the present invention;

Figure 8 illustrates a short message transmitted to a mobile station in accordance with the present invention;

Figure 9 illustrates functions carried out by a mobile station when displaying a cell broadcast message in accordance with the present invention;

15 Figure 10 shows an example of a display of a decrypted message in accordance with the present invention;

Figure 11 illustrates an example of a display of an encrypted message in accordance with the present invention; and

20 Figures 12 and 13 are flow diagrams illustrating encryption key updating procedures carried out in accordance with the present invention.

A GSM network, referred to as a public land mobile network (PLMN), is schematically illustrated in Figure 1. This is in itself known and will not be

described in detail. A mobile switching centre (MSC) 2 is connected via communication links to a number of base station controller (BSCs) 4. The BSCs 4 are dispersed geographically across areas served by the mobile switching centre 2. Each BSC 4 controls one or more base transceiver stations (BTSs) 6 located remote from, and connected by further communication links to, the BSC. Each BTS 6 transmits radio signals to, and receives radio signals from, mobile stations 8 which are in an area served by that BTS. That area is referred to as a "cell". A GSM network is provided with a large number of such cells, which are ideally contiguous to provide continuous coverage over the whole network territory. The radio signals are separated into a number of distinct communications channels. These include common channels and traffic channels. The traffic channels are used for point to point communications (voice calls, data calls, etc) with specific mobile stations. The common channels are received by all mobile stations being served by the cell and contain signalling and/or message data.

The mobile switching centre 2 is also connected via communications links to other mobile switching centres in the remainder of the mobile communications network 10, and to other networks such as a public service telephone network (PSTN), which is not illustrated. The mobile switching centre 2 is provided with a home location register (HLR) 11 which is a database storing subscriber authentication data including the international mobile subscriber identities (IMSI) which are unique to each mobile station 8. An

IMSI consists of a mobile country code (3 decimal digits), a mobile network code (2 decimal digits) and a mobile subscriber code (up to 10 decimal digits) identifying a subscriber within a particular network. The IMSI is also stored in the mobile station in a subscriber identity module (SIM) (to be described below) along with other subscriber-specific information.

5 The mobile switching centre is also provided with a visitor location register (VLR), not shown, which is a database temporarily storing subscriber authentication data for mobile stations active in its area.

10 In addition, the MSC is connected to a cell broadcast centre (CBC) 12 for originating cell broadcast (CB) messages in the network, a short message centre (SMC) 13 for handling the transfer of point to point short messages within the network, a network management centre (NMC) 14 for performing management functions in the network, and a customer services system (CSS) 15 for performing customer service functions, including the updating of customer 15 subscription data for example by manual input at workstations in the system.

Referring to Figure 2, a mobile station 8, more specifically a cellular mobile telephone, comprises a transmit/receive aerial 16, a radio frequency transceiver 18, a speech coder/decoder 20 connected to a loudspeaker 22 and a microphone 24, a processor circuit 26 and its associated memory 28, an LCD display 30 and a manual input port (keypad) 32. The mobile station 8 is connected to a removable SIM 34 via electrical contacts 35.

The SIM 34 connected to the mobile station has a SIM processor 36, for example a Hitachi H8 microprocessor, and SIM memory 38, which includes for example 16 kilobytes of mask-programmed ROM 38a containing the SIM operating system, 8 kilobytes of read/write EEPROM 38b for the non-volatile storage of data items and 256 bytes of RAM for use by the SIM processor 36 during operations.

As described above, the SIM 34 is used for the storage and retrieval of data items by the processor 26 of the mobile station 8. The command set, data file structure and data coding format for data communicated via the interface between the mobile station processor 26 and the SIM processor 36 are all specified, in GSM technical specification 11.11.

Referring back to the network elements illustrated in Figure 1, the CBC 12 holds a set of cell broadcast messages to be broadcast within the network, and transmits them to the BSCs 4 in accordance with location areas which are predefined for each message type. Each cell broadcast message is provided with a unique message identifier (a 16 bit integer), which identifies the type of the message. The BSCs 4 then proceed to broadcast the message, via the respective BTSs 6, on their CBCBs. The CBCB protocols and the timing of the broadcasts are specified in GSM technical specification 05.02.

The CBC 12 holds a list as illustrated in Figure 3, specifying encryption keys for each type of message which is to be broadcast in encrypted form. For each such message, the key is listed against the message identifier. Each key is

a 16 bit integer and, since the message identifiers are also 16 bit integers, no two keys in the list need to be the same. The keys are used to encrypt a message using an XOR function as will be described below.

Figure 4 illustrates a procedure carried out by the CBC 12 when receiving a new message for transmission as a cell broadcast message. A new message may be provided in the CBC 12 for example by manual input on a workstation associated with the CBC, or may be provided on-line from a remote source.

When the CBC 12 receives the new message, which may be an update of a previous message stored for the same message identifier, the message is stored by the CBC 12 and any previous message stored for the same message identifier is overwritten, step 50.

Next, the CBC 12 checks, using the message identifier provided with the new message, whether the message identifier appears in the key list illustrated in Figure 3. If no key is held for that particular message identifier, the message will be made generally available by cell broadcast to all mobile stations served in the cells in which the message is to be distributed. The message is transmitted for broadcast to the relevant BSCs 4 in unencrypted form, step 52.

The cell broadcast message may consist of one or more (up to a maximum of 15) pages. Each cell broadcast page consists of 88 octets of information, consisting of a 6 octet header and 82 octets for message text. A 7 bit default character set is used, equating to up to 93 characters per page.

Figure 5 illustrates the manner in which each page of a cell broadcast message is transmitted in a cell by the BSC/BTS on the CBCH. The broadcast is divided into four blocks per page. The first block 100 contains 2 octets of data 108 indicating the serial number for the page, 2 octets of data 110 indicating the message identifier for the page, 1 octet of data 112 identifying the coding scheme used for the message text, and 1 octet of data 114 indicating the page parameter. The remaining 16 octets of data 116 contain the first part of the message text for the page.

The remaining 3 blocks 102, 104, 106 of the page broadcast consists entirely of message text, except each block is headed by a single octet of data 118 indicating the block type.

The serial number indicated in block portion 108 is a 16 bit integer which is used to identify a particular message. The serial number is updated when a message with a given message identifier is updated. The serial number consists of a 12 bit message code and a four bit update number, which are incremented according to message updates.

The message identifier in portion 110 is used to identify the type of message, as described above.

The coding scheme indicated in portion 112 is used to indicate the source language of the message, allowing a user to screen out any messages received in a language in which they are not conversant. The page parameter

indicated in portion 114 is used to specify the current page number within a message and the total number of pages within the message.

The message text for each page consists of up to 93 characters. If the message text within a page is shorter than 93 characters in length, the carriage return (CR) character is used to provide packing, thus bringing the total number of characters to 93. To maintain an integral number of octets, the remaining 5 bits are set to "0" as padding data at the end of the page.

The block structure illustrated in Figure 5 is that of a conventional cell broadcast message, and may be received and displayed by currently-available GSM-type mobile stations in receipt of the cell broadcast channel on which the message is broadcast.

Referring again to Figure 4, if on the other hand the CBC 12 detects the message identifier of the new message in the key list, the corresponding key is retrieved, step 54. The key is then used to encrypt the message, step 56, which is then transmitted to the appropriate BSCs 4, step 58. The encryption of step 56 is performed by applying an XOR function between the most significant 8 bits of the key and each odd-numbered message text octet in a page, and by applying the XOR function between the least significant 8 bits of the key and each even-numbered message text octet in a page, except the last such octet.

The pages broadcast by the BSCs 4 when receiving encrypted cell broadcast messages are of the form illustrated in Figure 6. Each page consists of the same components as the unencrypted page illustrated in Figure 5, namely

4 blocks each containing the various header portions. However, the majority of the message text is encrypted, as indicated by shading in Figure 6. The last octet of each page of message text, which contains the 5 bits of padding data, is left unencrypted, in order to protect the integrity of the padding data, which would be lost if encrypted. Each of the header portions is also transmitted in unencrypted form, to allow the proper reception and reading of the data in the header portions by all mobile stations 8.

In order to properly receive and present an encrypted cell broadcast message in intelligible form to a user, a mobile station 8 must be provisioned with the decryption key corresponding with the encryption key used to encrypt the message. With the XOR function as the encryption function, the encryption/decryption process is symmetric, and the same key used to encrypt the message is used to decrypt the message. This key is referred to herein as an encryption key when to be used to encrypt data, and a decryption key when to be used to decrypt data.

In order to provision the mobile station 8 with the decryption key, a remote provisioning procedure is used, involving a remote SIM updating (RSU) message being transmitted to the mobile station 8, such as described in European patent application no. EP-A-0562890, the contents of which are incorporated herein by reference, or using the "data download via SMS Point-to-point" (SMS-PP data download) procedure as described in GSM Technical Specification 11.14, "Specification of the SIM Application Toolkit for the

Subscriber Identity Module - Mobile Equipment (SIM-ME) Interface". The decryption keys are transmitted using a point-to-point data transfer protocol, such as the GSM-defined Short Message Service (SMS), over the radio interface to the mobile station 8 for storage in the SIM 34. The SIM 34 is provided with a cell broadcast decryption keys data field dedicated to the storage of cell broadcast decryption key data.

Figure 7 illustrates the procedures carried out by the NMC 14 in order to provision the mobile station 8 of a particular subscriber with decryption keys for each limited-access message type which the subscriber is entitled to have access to. The CSS 15 holds a record for the subscriber, indicating the access rights for that subscriber. These access rights are indicated by including in the subscriber record a list of the appropriate message identifiers for the message types which the subscriber should have access to. This access rights list may be updated and changed in the CSS 15.

In order to provision the mobile station 8 of the subscriber, the NMC 14 first interrogates the CSS 15 to determine the message access rights which are held for the subscriber, step 60. The NMC 14 also interrogates the HLR 11 in order to retrieve the IMSI of the subscriber, step 62. The NMC 14 also interrogates the CBC 12 to retrieve the decryption keys corresponding to each of the message identifiers indicated in the access rights details returned by the CSS 15, step 64. Next, each of the decryption keys returned by the CBC 12 is then itself encrypted by applying the XOR function between the 16 bits of the

decryption key and 16 predetermined bits of the subscriber's IMSI record, step 66. This is to ensure that the decryption key may only be used by a mobile station 8 having access to the subscriber's IMSI (which is stored in the subscriber's SIM 34).

5 Once the decryption keys are encrypted, the NMC 14 forwards an RSU message to the SMC 13 for transmission, via the radio interface, as an SMS message to the mobile station 8 of the subscriber. The SMS message is transmitted conventionally, via a dedicated data channel, to the mobile station 8. The RSU message has the form illustrated in Figure 8, and includes a header 10 portion 70, the message identifiers for each message type to which the subscriber should have access to, the encrypted decryption keys, and alpha tags (alphanumeric identifiers) for use by the subscriber to readily identify each of the message types. The header portion 70 includes a flag indicating that the SMS message is an RSU message, and a command indicating that the contents 15 of the message are to be stored in the cell broadcast decryption keys data field.

On receipt of the SMS message, the mobile station forwards it for storage as an SMS message to the SIM 34. However, since the message has an RSU flag, the SIM processor 36 notes that the message is an RSU message, and updates the cell broadcast decryption keys data field in the SIM 34 with the 20 message identifiers, the corresponding encrypted keys, and the corresponding alpha tags contained in the RSU message. The mobile station is now provided with the capability to decrypt all encrypted cell broadcast messages having

message identifiers corresponding to those stored in the cell broadcast decryption keys data field.

A user of the mobile station may, by appropriate keystrokes on the keypad 32, select cell broadcast messages which the mobile station is to pick up and store for possible display by the user. The user may display the alpha tags for the message types of limited access messages, in order to aid the selection of the limited access message types which the user wishes to have displayed. The user is also able to select the message identifiers for message types of general access messages, and for message types of limited access messages which the mobile station has no decryption keys.

When a cell broadcast message is received by the mobile station 8 which has a message identifier of the type selected for possible display by the user, and no message is yet stored for the message identifier, the mobile station 8 picks up the message and stores the message in a cell broadcast message data field provided in the SIM 34. If the SIM 34 already has a message stored for the message identifier in the cell broadcast message, the mobile station 8 checks the serial number of the message to determine whether it has been updated. If so, the mobile station overwrites the previously-stored message in the SIM 34 with the updated message. Otherwise, the mobile station 8 ignores the contents of the cell broadcast message.

When a cell broadcast message is newly picked up and stored, the user is prompted, for example by an audio tone or by a particular icon on the LED

display 30 of the mobile station 8, to indicate that a cell broadcast message is ready to be displayed. The mobile station then performs the procedures illustrated in Figure 9.

The mobile station first waits for input by the user requesting the 5 message to be displayed. On receipt of such input, the mobile station checks whether it is currently camped on its home network (HPLMN). If the mobile station is camped on a network which is not its home network, the mobile station proceeds directly to display the stored message. If the message is encrypted, the encrypted message is displayed in a form unintelligible to the 10 user, step 78, as the message is of the limited access type and access to the information is denied to the subscribers of other networks. If the message however is unencrypted, i.e. of the general access type, the message is displayed in an intelligible form, step 80.

If the mobile station is camped on its home network, the mobile station 15 checks whether the SIM 34 has the cell broadcast decryption keys data field provided in accordance with this invention. If not, the mobile station proceeds once again to either display an encrypted message, step 78, or an intelligible message, step 80, depending on the access type of message broadcast.

If the SIM 34 currently in the mobile station does have the cell broadcast 20 decryption keys data field, the mobile station proceeds to interrogate the SIM 34 to check whether the message identifier of the stored message is present in the cell broadcast decryption keys field. If not, the message received may be of a

general access type, and the message is displayed by the mobile station 8 in intelligible form, step 80. Otherwise, the message is of a limited access type to which the user has no access rights. The message is then displayed by the mobile station 8 in encrypted, i.e. unintelligible form, to prevent receipt of the information in the message by the user, step 78.

If the message identifier of the stored message is present in the cell broadcast decryption keys data field on the SIM 34, the mobile station 8 proceeds to retrieve the encrypted decryption key corresponding to the message identifier of the stored message, along with the subscriber's IMSI, from the SIM, step 82.

With the encrypted decryption key and the IMSI, the mobile station 8 performs the reverse of the encryption process carried out in the NMC 14, to obtain the original decryption key, step 84. This decryption is carried out by performing an XOR function between the 16 bits of the encrypted decryption key and the same set of 16 predetermined bits from the subscriber's IMSI used in the encryption process.

The mobile station 8 then proceeds to decrypt the stored message, by performing the reverse of the encryption process carried out in the CBC 12 when generating the encrypted cell broadcast message. Namely, the mobile station performs the XOR function between the 8 most significant bits of the decryption key and each odd-numbered message text octet, and between the 8 least significant bits of the decryption key and each of the even-numbered

message text octets, except for the last octet in each page (which was originally not encrypted). This returns the original cell broadcast message text, which is then displayed on the LCD display 30 of the mobile station, step 88, in a form intelligible to the user.

5 Figure 10 illustrates an example of an original cell broadcast message, consisting of one page containing 89 message text characters and 4 carriage return (text padding) characters. This message is encrypted as described in relation to Figure 4, and after receipt and storage by the mobile station may be displayed in accordance with the procedure shown in Figure 9.

10 If the mobile station has been provisioned with the corresponding decryption key, the message may be displayed in its original form as illustrated in Figure 10.

15 If however the mobile station has not been provisioned with the appropriate decryption key, the message will appear as illustrated in Figure 11, as a pseudo-random character set.

Because the number of bits of the encryption key is not equal to, nor a multiple of, the number of bits used per character in coding the text, there is no direct correspondence between any one of the original characters and the characters displayed in the encrypted text. In this case, the coding scheme used for the text characters utilises 7 bits per character, and the encryption keys contain 16 bits. Of course, other combinations of text character coding length and encryption key length may be used to similar effect.

To ensure the long-term security of the encryption method used for limited access messages, the encryption keys used to encrypt the message texts will periodically be altered. Figure 12 illustrate a procedure carried out by the CBC 12 to update a particular encryption key. The CBC 12 first randomly generates a new 16 bit encryption key, step 90, and overwrites the previously-stored encryption key in the list illustrated in Figure 3 for the message identifier in question, step 91. Next, the CBC 12 proceeds to retrieve the message previously stored for the message identifier in question, step 92, and proceeds to encrypt the message with the newly generated encryption key, step 93. This encryption process is identical to that carried out when the message was originally received by the CBC 12 as described in relation to Figure 4, of course using a different encryption key. Once the message is encrypted, the new cell broadcast message is forwarded to the appropriate BSCs 4, step 94, for broadcast by the BTSs 6 on their CBCHs to mobile stations 8 receiving the cell broadcast channel in the cells served by the BSCs 4 in question.

Once a new encryption key has been generated in the CBC 12, and the corresponding cell broadcast message has been encrypted with the newly-generated key, the mobile stations 8 of users having access rights to the same message type must be provisioned with the new decryption key.

The first step of provisioning the mobile stations 8 of the appropriate subscribers with new decryption keys generated in the CBC 12 is the procedure carried out in Figure 13. First, the CSS 15 receives from the CBC 12 a list of

message identifiers for the messages for which the decryption keys have been updated, step 95. The CSS 15 then proceeds to search its store of subscription records for the message identifiers on the updated decryption keys list, in order to determine which subscriptions require updated decryption keys, step 96. The  
5 CSS 12 then constructs a list of such subscriptions, which are forwarded to the NMC 14 to allow the NMC 14 to perform the appropriate provisioning procedures, step 97. The NMC 14 then proceeds to perform the procedure described in relation to Figure 7 for each subscription appearing on the list received from the CSS 15. This results in the mobile stations of each such  
10 subscription receiving a new RSU message containing updated decryption keys, in encrypted form, for message types to which the subscriber has access. These decryption keys are suitable for use in decrypting messages encrypted with the newly-generated encryption keys.

The encryption/decryption mechanism utilised in the above-described embodiment utilises the two-way encryption/decryption character of the XOR function, and is sufficiently secure for use in relation to many types of information. However, it will be appreciated that other two-way encryption/decryption mechanisms, for example using symmetric or public/private encryption/decryption keys, may be utilised to provide more (or less) secure  
20 encryption/decryption mechanisms.

In the above-described embodiment, the general-access messages are not subject to the XOR function used in the encryption/decryption process.

However, it would also be possible to subject the message to the XOR function using a "free" key of the form of 16 bits of "0", which results in a message coding which is identical to the original message coding. This XORing with the "free" key may be performed in the CBC 12 when "encrypting" a general access message, and/or by the mobile station 8 when "decrypting" a general access message. In effect, no encryption or decryption would take place.

5

In the above-described embodiment, the mobile station 8 performs the decryption of the cell broadcast message text. This requires the mobile station itself to be customised, in relation to currently existing mobile station types, in order to allow the mobile station to present the encrypted cell broadcast messages in plain text form. In a further embodiment, a standard mobile station, such as a GSM (Phase 2+) mobile station supporting the SIM Toolkit as described in GSM Technical Specification 11.14, may be used. In this further embodiment, the functionality for decrypting encrypted cell broadcast messages 10 is contained in the SIM 34 itself, the SIM 34 being SIM Toolkit enabled.

10

15

20

In order to avoid repetition, it should be understood that the functionality described in relation to each of Figures 3, 4, 7, 8, 12 and 13 is intended to apply equally in relation to 13. This embodiment differs primarily from the first-described embodiment in that the special cell broadcast coding scheme illustrated in Figure 6 is not necessary, a conventional "data download via SMS-CB" coding scheme being used instead, and in that the procedure illustrated in Figure 9 is not carried out by the mobile station, the mobile station

instead passing "data download via SMS-CB" messages directly to the SIM, and subsequently being instructed by the SIM (the SIM being proactive) to display a plain text version of a cell broadcast message received in encrypted form.

5 Referring to Figure 4, in this embodiment any suitable type of encryption technique may be used in step 56. This may be the XOR function previously described, or other encryption techniques such as DES, RSA, etc.

10 In place of the coding scheme illustrated in Figure 6, in this embodiment each of the BSCs 4 broadcasting encrypted cell broadcast messages formats the encrypted message as a "data download via SMS-CB" message, the encrypted message being included in the cell broadcast page along with an identifier for the key used to encrypt the message. The cell broadcast message includes a cell broadcast message identifier, which specifies the type of content contained in the cell broadcast page, and a transfer protocol identifier indicating that the 15 message type is "SIM data download".

20 In addition to the field dedicated to containing decryption keys, which may be populated by means of RSU procedures as described above, the SIM 34 contains a Cell Broadcast Message Identity for Data Download (CBMID) data field, as described in GSM Technical Specification 11.11, which holds data identifying the message content types the subscriber wishes the mobile station 8 to accept. Furthermore, the SIM 34 includes an application programme, which

may for example be stored in ROM or EEPROM on the SIM, for performing decryption and controlling the display of the mobile station 8.

When the mobile station receives the cell broadcast download message, the mobile station 8 first queries the CBMID data field of the SIM to determine whether the message ID received for the cell broadcast message is currently selected by or for the subscriber. If a corresponding entry is found in the CBMID data field, the mobile station 8 transparently passes the cell broadcast page to the SIM 34 using a "cell broadcast download to SIM" command.

Reception of the cell broadcast download command by the SIM 34 causes the SIM to analyse the contents of at least a portion of the cell broadcast page, wherefrom it is determined whether the cell broadcast page contains an encrypted message. If so, the stored programme is invoked in order to decrypt the message, using the appropriate decryption key stored in the dedicated decryption keys field. Once the message is decrypted, the SIM passes the plain text message to the mobile station in a "display text" command, in response to which the mobile station 8 displays the plain text message.

In addition to decrypting the encrypted message and commanding the mobile station 8 to display the plain text message, the SIM application programme may also perform other processes in response to data received in the cell broadcast message, such as updating the contents of the CBMID data field to select new message types, on behalf of the subscriber, which the mobile station 8 should accept and handle.

As will be appreciated, in this embodiment, if a subscriber is not authorised to receive a limited access message in plain text form, the SIM may either not contain an appropriate decryption key for the message or may be at least temporarily configured by the network operator so as not to conduct the procedure described above. Instead of the procedure described above, the SIM may act in one of a variety of alternative manners. For example, the SIM may command the mobile station 8 either to present the message to the user in encrypted form or to display an access-denied message, or may simply not any display on the mobile station, in response to a cell broadcast message containing an encrypted message which is of a type nevertheless selected by the subscriber.

The functionality for the provision and processing of encrypted cell broadcast messages may thus be contained entirely within the mobile communications network and on the SIM 34, and standard (e.g. GSM Phase 2+) handsets may be used without modification.

It will be appreciated that various modifications and variations may be employed in relation to the above-described embodiments.

The provisioning of the mobile stations with decryption keys via the air interface, using the RSU-type short messages, has the advantage that no action is required on the subscriber's behalf in order to provision the SIM 34 of the mobile station 8 with the decryption keys. However, the decryption keys, preferably encrypted using the subscriber's IMSI, or such like, as described, may be transmitted to the user by other methods, for example by mail. An

alternative functionality of the mobile station 8 would allow the encrypted decryption keys to be manually input to the mobile station for storage in the cell broadcast decryption keys data field in the SIM 34.

Other information access prevention mechanisms to those described 5 above could also be employed, such as the remote enablement/disablement(for example using RSU messages) of a decryption function on the mobile station, or of the cell broadcast receiving function on the mobile station.

In the above-described embodiments, the SIM 34 is in the form of a 10 module electrically connected to the mobile station 8. However, the SIM may be embodied in an entirely separate module, such as a contactless smartcard transmitting data to and from the mobile station via a radio link.

Finally, although the above-described embodiments relate to a method and apparatus utilised in a GSM-type network, the present invention may of course be realised in other types of cellular telecommunications networks, 15 whether using TDMA, CDMA, or other types of radio interface protocols.

It is envisaged that further modifications and variations may be employed without departing from the scope of the present invention.

ART 34

CLAIMS

1. A method of distributing information to users in a cellular telecommunications network comprising a plurality of base stations transceiving in a plurality of cells of said network, said method comprising:

5 providing a plurality of mobile stations, each of said mobile stations having an associated information access status;

10 broadcasting a signal on a common channel of at least one cell of said network, said signal containing a limited access message in encrypted form, for general reception in said at least one cell;

15 enabling first mobile stations having a first information access status to decrypt and present said message to a user in unencrypted form when being served by said cell; and

20 preventing second mobile stations having a second information access status from presenting said message in unencrypted form to a user when being served in said cell,

wherein said first mobile stations are provided with a removable module which may be used in association with any of a plurality of mobile stations, said removable module storing a decryption key for said message,

25 and wherein said message is decrypted, using said decryption key, in said removable module.

AMENDED SHEET

2. A method according to claim 1, wherein said signal comprises a message identifier accompanying a message and said method comprises enabling both said first and second mobile stations to read said message identifier.

5

3. A method according to claim 1 or 2, wherein said decryption key is stored in said removable module in encrypted form.

4. A method according to claim 3, wherein said decryption key is 10 decrypted by said first mobile station using a data string specific to said removable module.

5. A method according to claim 4, wherein said data string is a subscriber identifier used in said cellular telecommunications network.

15

6. A method according to any preceding claim, further comprising transmitting said decryption key to said first mobile stations via a radio interface in said cellular telecommunications network.

20

7. A method according to any preceding claim, wherein said removable module is a subscriber identity module.

AMENDED 3 LINES

8. A method according to claim 7, wherein said message includes a transfer protocol identifier indicating that the message is of a type for data download to the subscriber identity module from the mobile station.

5 9. A method according to any preceding claim, wherein said removable module stores an application programme for performing the decryption and for controlling a display of said message on the mobile station.

10. A method according to any preceding claim, wherein said signal  
10 comprises a plurality of limited access messages each having a corresponding  
decryption key.

15 said method comprising providing said first mobile stations with said decryption keys, storing said decryption keys on removable modules of said first mobile stations, and enabling only ones of said first mobile stations having a decryption key corresponding to a limited access message to present said limited access message to a user in unencrypted form when being served in said cell

11. A method according to claim 10, comprising providing each of  
20 said first mobile stations with a selection of said subscription keys in accordance  
with a subscription held for each first mobile station respectively.

12. A method according to any preceding claim, wherein alternative limited access messages are broadcast in cells located in different areas of said cellular telecommunications network.

5 13. A method according to any preceding, wherein said common channel is a cell broadcast channel of a GSM-type communications system.

14. A mobile station for receiving information in a cellular telecommunications system, said mobile station comprising:

10 means for receiving an encrypted message broadcast on a common channel of a cell of said cellular telecommunications system; and

means for displaying said message, when decrypted, to a user; and  
a removable module comprising a memory for storing a decryption key,  
and means for decrypting said message using said stored decryption key.

15

15. A mobile station according to claim 14, wherein said removable module is a subscriber identity module.

20 16. A mobile station according to claim 14 or 15, wherein said removable module stores an application programme for performing the decryption and for controlling the display of said message on the mobile station.

17. A GSM Phase 2+ mobile station according to any of claims 14 to 16.

5 18. A cellular mobile telephone according to any of claims 14 to 17.

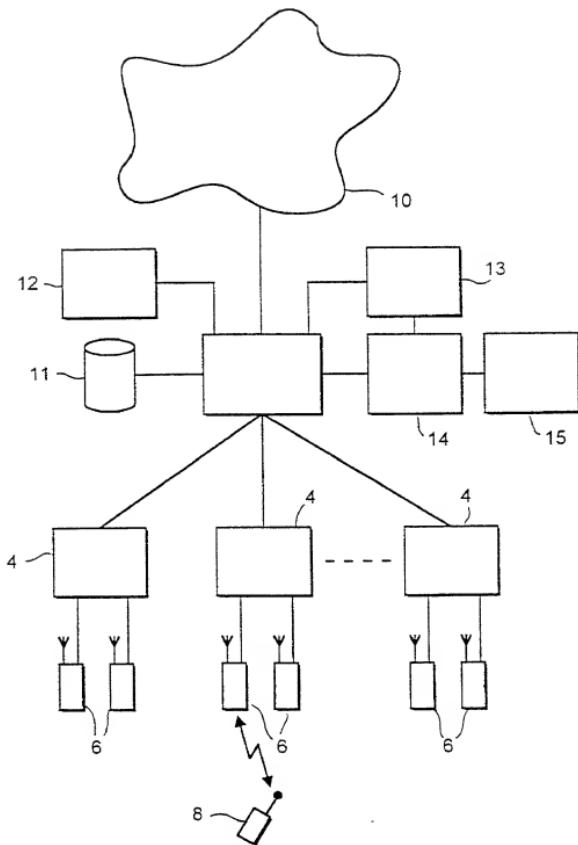


FIG. 1

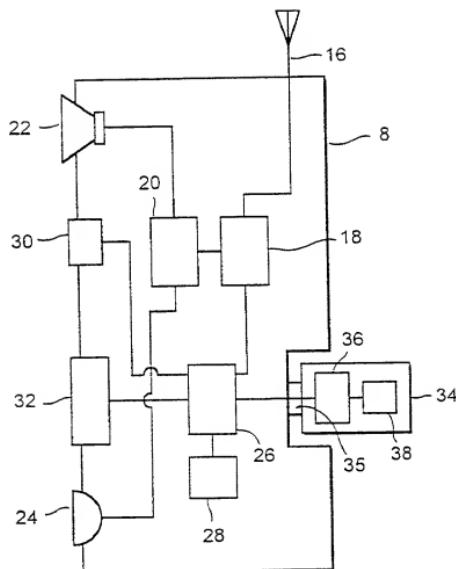


FIG. 2

MESSAGE IDENTIFIER	KEY
-----	-----
-----	-----
⋮	⋮
-----	-----

FIG. 3

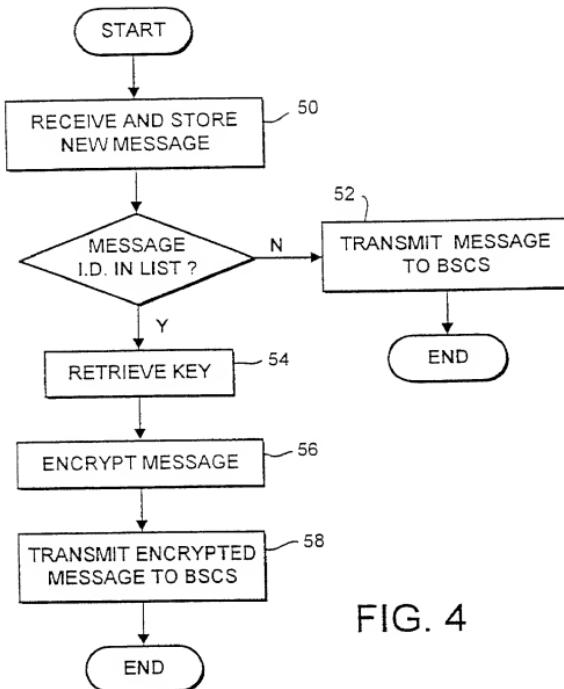


FIG. 4

4 / 8

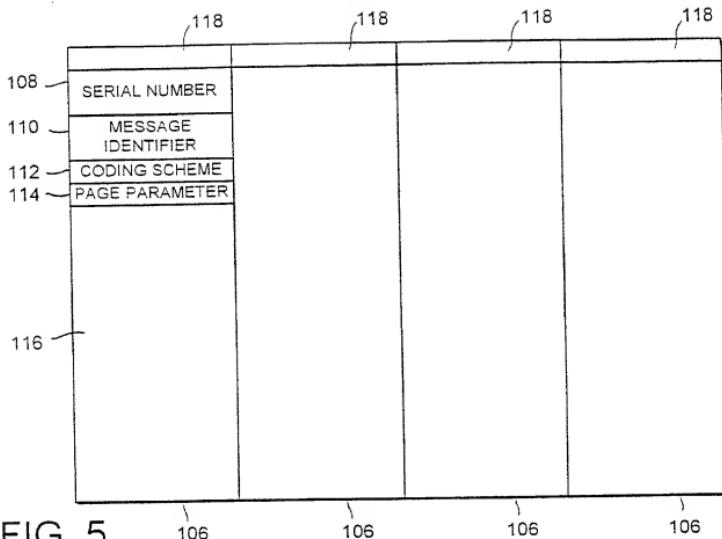


FIG. 5

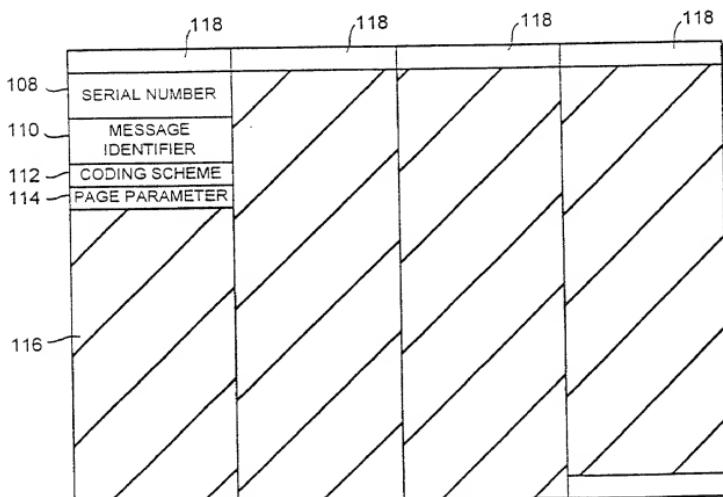


FIG. 6

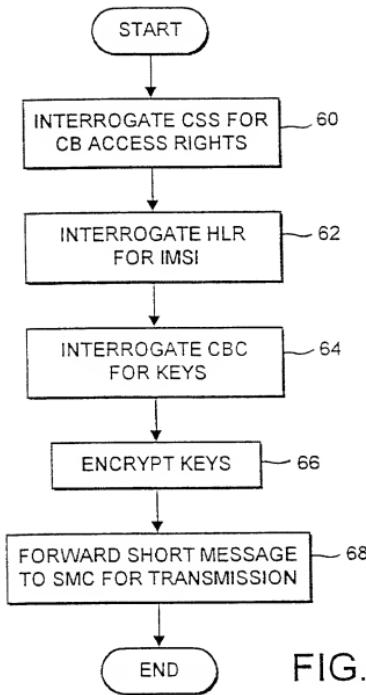


FIG. 7

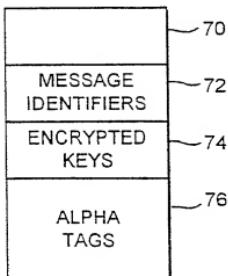


FIG. 8

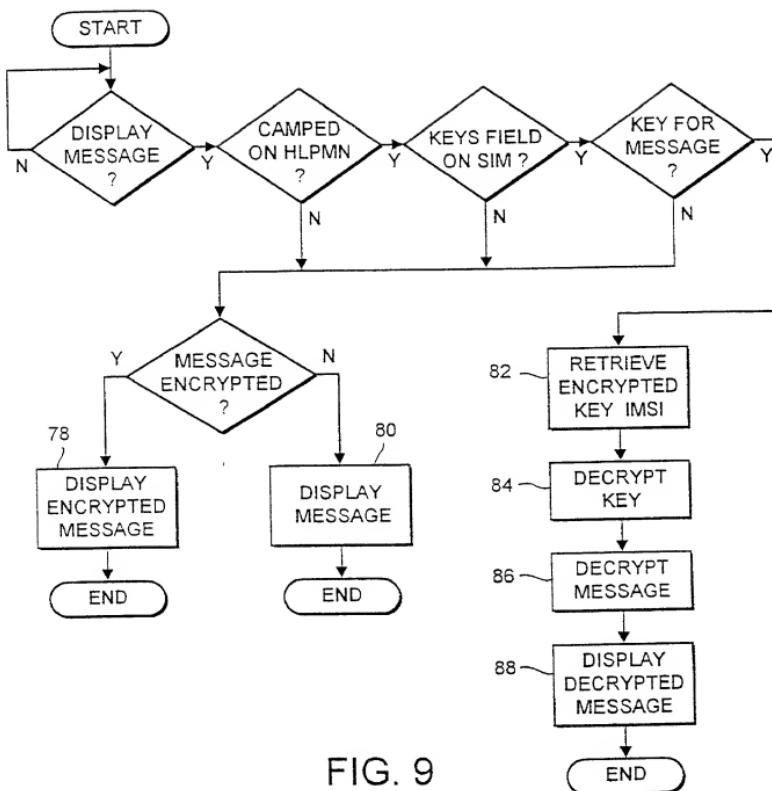


FIG. 9

T	h	i	s	i	s	a	n	e	x	a	m	p	l	e	o	f	h	o	w	S	M	S	
C	B	m	e	s	s	a	g	e	s	s	h	a	l	l	b	e	c	o	d	e	d	.	
I	"	0	4	5	4	6	2	4	8	2	3	"	F	o	r	m	o	r	e	i	n	f	o
CR	CR	CR	CR																				

FIG. 10

0	s	U	æ	ö	P	©	F	.	u	Ψ	Φ	□	X	β	Π	l	ü	Ψ	£	:	0	NU	§	:
0	□	m	v	R	æ	/	X	Δ	¥	>	;	F	ü	=	U	6	/	ü	Ψ	CR	3	N	Δ	\$
0	0	Q	V	y	0	¥	X	n	CR	K	V	ü	9	Ψ	ò	3	K	S	Φ	"	1	R	N	5
:	c	\$																			W	Ω	ç	C

FIG. 11

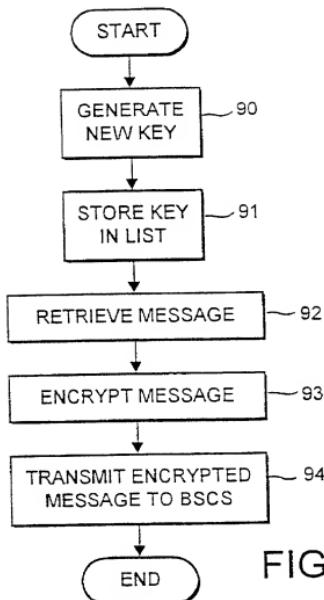


FIG. 12

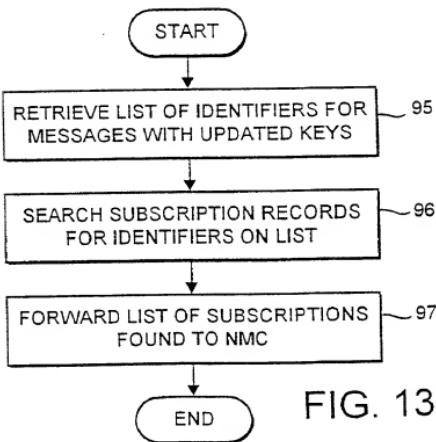


FIG. 13



## COMBINED DECLARATION FOR PATENT APPLICATION

As the below named inventor, we hereby declare that:

Our residence, post office address and citizenship are as stated below next to our names;

We believe we are the original, first and joint inventors of the subject matter which is claimed and for which a patent is sought on the invention entitled: ENCRYPTED BROADCAST MESSAGES IN A CELLULAR COMMUNICATIONS SYSTEM.

the specification of which

is attached hereto.  
 was filed on \_\_\_\_\_ as Application Serial Number \_\_\_\_\_ and was amended on \_\_\_\_\_ (if applicable).

was described and claimed in PCT International Application No. PCT/GB98/02064 filed on 13 July 1998 and was amended under PCT Article 19 on \_\_\_\_\_ (if applicable).

We hereby state that we have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

We acknowledge the duty to disclose information which is material to patentability in accordance with Title 37, Code of Federal Regulations, § 1.56(a).

We hereby claim foreign priority benefits under Title 35, United States Code, § 119 of any foreign application(s) for patent, design or inventor's certificate or of any PCT international application(s) listed below and have also identified below any foreign application(s) for patent, design or inventor's certificate or any PCT international application(s) designating at least one country other than the United States of America filed for the same subject matter having a filing date before that of the application of which priority is claimed:

#### Prior Foreign Application(s)

Country	Application Number	Date of Filing (day, month, year)	Date of Issue (day, month, year)	Priority Claimed Under 37 U.S.C. § 119
GB	9715097.3	17 July 1997		YES

#### Prior United States Application(s)

We hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, we acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

Application Serial Number	Date of Filing (Day, Month, Year)	Status — Patented, Pending, Abandoned

We hereby declare that all statements made herein of our own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

Signature   
Full Name of  
First Inventor FORD Family Name Peter First Given Name  Second Given Name  
Residence Bristol, United Kingdom. GBX  
Citizenship British.  
Post Office  
Address 18 Summers Mead, Yate, Bristol, BS17 5RB, United Kingdom.

0001474634456000